REMARKS

Claims 1-5, 7-13, 15-20, and 22-24 were pending and stand rejected. Claims 1, 9, 16, and 23 have been amended. New claims 25-26 have been added. Claims 1-5, 7-13, 15-20, and 22-26 are pending upon entry of this amendment.

On June 6, 2007, the Examiner left a voicemail for the undersigned attorney about an Information Disclosure Statement that was mailed by Applicant on August 17, 2006 and received by the Patent Office on August 22, 2006. The Examiner stated that he would consider the references cited therein and send Applicant an initialed Form 8A with the next office communication. The initialed Form 8A was not sent with the next office communication. **Applicant requests that the Examiner consider the references cited therein and send Applicant an initialed Form 8A with the next office communication.**

The specification and FIG. 2 have been amended to correct typographical errors. No new matter has been added by these amendments.

Claims 1-3, 5, 7-11, 13, 15-18, 20, and 22-24 were rejected under 35 USC 103(a) as being unpatentable over Porras in view of Pifer. Applicant respectfully traverses. As amended, claim 1 recites in part:

> determine, based on the first alert and the second alert, whether the first clock and the second clock are synchronized; and
> if the first clock and the second clock are not synchronized:
> synchronize the first clock and the second clock;
> modify at least one of a timestamp within the first alert and a timestamp within the second alert; and
> correlate the first alert and the second alert according to a rule.

As described in the pending application, the claimed invention comprises a first software agent, a second software agent, and a manager module (¶¶12-15; FIG. 1). The manager module receives a first stream of alerts from a first network security device having a first clock and a

second stream of alerts from a second network security device having a second clock (¶22). The manager module identifies a first alert in the first stream and a second alert in the second stream, wherein the first alert includes an Internet Protocol (IP) address, and wherein the second alert includes the IP address (¶¶23-24). The manager module determines, based on the first alert and the second alert, whether the first clock and the second clock are synchronized (¶26). If the first clock and the second clock are not synchronized, the manager module synchronizes the first clock and the second clock (¶26), modifies at least one of a timestamp within the first alert and a timestamp within the second alert (¶36), and correlates the first alert and the second alert according to a rule (¶¶23, 36, 14; FIG. 1).

Applicant agrees with the Examiner that Porras does not disclose, teach, or suggest determining, based on a first alert and a second alert, whether a first clock and a second clock are synchronized. Also, while Porras mentions in passing the existence of a system clock (6:55-57), it does not disclose, teach, or suggest synchronization of clocks or modification of timestamps. It follows that Porras does not disclose, teach, or suggest the claimed element "correlate the first alert and the second alert according to a rule" after "modify[ing] at least one of a timestamp within the first alert and a timestamp within the second alert."

Pifer does not remedy this deficiency. Pifer discusses a synchronization system and method for a lightning location system having a plurality of remote lightning detectors transmitting data to a lightning position analyzer (Abstract). Each of the detectors includes a clock for identifying the time of occurrence of a detected lightning discharge (3:34-36). The position analyzer correlates the data from two or more detectors and synchronizes the detectors utilizing the lightning discharge itself as an external time reference (3:52-56).

Pifer does not disclose, teach, or suggest the claimed element "correlate the first alert and the second alert according to a rule" after "modify[ing] at least one of a timestamp within the first alert and a timestamp within the second alert," as claimed. In Pifer, the difference between the times of occurrence as measured by the first and second detectors for the lightning event is calculated and used to correct the time of occurrence data for each lightning event detected by the second detector (4:35-40). However, Pifer does not teach or disclose that after correcting the time of occurrence data, two alerts are correlated as claimed.

Thus, claim 1 (as amended) is patentable over Porras and Pifer, both individually and in combination. Independent claims 9, 16, and 23 (as amended) recite similar language and are also patentable over Porras and Pifer, both individually and in combination, for at least the same reasons.

Claims 4, 12, and 19 were rejected under 35 USC 103(a) as being unpatentable over Porras in view of Pifer further in view of Apel. Applicant respectfully traverses. For the record, Applicant also traverses the Examiner's assertions regarding the disclosure of Apel and regarding the motivation to combine Porras and Pifer and Apel.

The claims not specifically mentioned above depend from claims 1, 9, 16, or 23 (directly or indirectly), which were shown to be patentable over Porras in view of Pifer. In addition, these claims recite other features not included in claims 1, 9, 16, or 23. Thus, these claims are patentable over Porras in view of Pifer, for at least the reasons discussed above, as well as for the elements that they individually recite.

Applicant respectfully submits that the pending claims are allowable over the cited art of record and requests that the Examiner allow this case. The Examiner is invited to contact the undersigned in order to advance the prosecution of this application.

Respectfully submitted,

HUGH S. NJEMANZE

Dated: January 9, 2008

By: /Sabra-Anne R. Truesdale/

Sabra-Anne R. Truesdale
Reg. No. 55,687
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel.: (650) 335-7187
Fax.: (650) 938-5200